RECAP:

POLYNOMIALS : $f = \sum_\alpha a_\alpha \mathbf{x}^\alpha$ $\quad f \in \mathbb{Q}[x_1, \dots, x_n]$

$\alpha \in \mathbb{Z}^n_{\geq 0}$ $\quad a_\alpha \in \mathbb{Q}$

MONOMIALS : $\mathbf{x}^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ $\quad$ multi-degree

total degree : $d = \alpha_1 + \dots + \alpha_n$

Polynomials can't be in general divided

Monomial ordering - Lexicographic, Graded reverse Lex ordering

Leading term : $LT(f) = LC(f) \cdot LM(f)$

leading coefficient $\quad$ leading monomial

$LC(f) = a_{\text{multideg}(f)}$ $\quad LM(f) = x^{\text{multideg}(f)}$

$\text{multideg}(f) = \max_{>} \{ \alpha \in \mathbb{Z}^n_{\geq 0} \mid a_\alpha \neq 0 \}$

Division theorem + algorithm

$>$, f, $F = (f_1, \dots, f_s)$: $\quad f = a_1 f_1 + \dots + a_s f_s + r$

$a_i, r \in \mathbb{Q}[x_1, \dots, x_n]$, either $r = 0$ or none of the monomials is divisible by any of $LT(f_1), \dots, LT(f_s)$

Furthermore $a_i f_i \neq 0 \Rightarrow \text{multideg}(f) \geq \text{multideg}(a_i f_i)$

One non-linear polynomial eq. in one unknown

- is well understood
- the problem can be fomulated as a computation of eigenvalues of a matrix
- Simple example

$$f = x^3 - 6x^2 + 11x - 6 = 0$$

We can construct a companion matrix

$$M_x = \begin{bmatrix} 0 & 0 & 6 \\ 1 & 0 & -11 \\ 0 & 1 & 6 \end{bmatrix}$$

the characteristic polynomial of M_x is

$$\det(M_x - xI) = \det\begin{pmatrix} x & 0 & -6 \\ -1 & x & 11 \\ 0 & -1 & x-6 \end{pmatrix} = x^3 - 6x^2 + 11x - 6 = f$$

$$= \det(xI - M_x)$$

Therefore eigenvalues of M_x $(1, 2, 3)$ are the solutions to $f(x) = 0$

Linear mapping represented by a matrix $M \in \mathbb{R}^{n \times n}$

Eigenvalues:

$$Mx = \lambda x$$

$$Mx - \lambda x = 0$$

$$Mx - \lambda I x = 0$$

$$(M - \lambda I)x = 0$$

$$x \neq 0 \Rightarrow \Updownarrow$$

$$\operatorname{rank}(M - \lambda I) < n$$

$$\Rightarrow \det(M - \lambda I) = 0$$

- This procedure applies in general when the coefficient at the monomial of f with the highest degree is equal to 1 (when we normalize the equation)
- Obviously such normalization using division by a non-zero coefficient at the monomial of the highest degree produces an equivalent equation with the same solutions

The general rule for constructing the companion matrix M_x for polynomial

$$f = x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

$$M_x = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ \vdots & & & \vdots & \\ 0 & \dots & \dots & 1 & -a_{n-1} \end{bmatrix}$$

Note that the eigenvalue computation must be in general approximate in general, roots of polynomials of degrees higher than 4 can't be expressed as finite formulas in coefficients a_i using $+, \cdot, \sqrt{\ }$

System of linear polynomial equations in several unknowns

Consider the following system of 3 linear polynomial equations in 3 unknowns

$$2x_1 + x_2 + 3x_3 = 0$$
$$4x_1 + 3x_2 + 2x_3 = 0$$
$$2x_1 + x_2 + x_3 = 2$$

and we write it in the standard matrix form

$$\begin{bmatrix} 2 & 1 & 3 \\ 4 & 3 & 2 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 2 \end{bmatrix}$$

Using Gassian elimination, we obtain an equivalent system

$$\begin{bmatrix} 2 & 1 & 3 \\ 0 & 1 & -4 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$$

We see that the system has exactly one solution

$$x_1 = \frac{7}{2}, \quad x_2 = -4, \quad x_3 = -1$$

- The key point of this method is to produce a sytem in a "triangulate shape" such that there is an equation in a single unknown (x_3), an equation in two unknowns ($f_2(x_2, x_3)$) and so on

- We can solve for x_3 and then transform f_2 by a substitution into an equation in a single unknown and solve for x_2 and so on

$$x_3 + 1 = 0 \quad , \quad x_2 - 4x_3 = 0 \quad , \quad 2x_1 + x_2 + 3x_3 = 0$$

is a so-called Gröbner basis

- Note that if we reorder unknowns we get a different GB

We can go even further and compute the reduced-row Echelon form form of this system

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \frac{7}{2} \\ -4 \\ -1 \end{bmatrix}$$

In this case we obtained so-called reduced GB

For a linear system with one solution there is a unique reduced GB for all orderings

In general (for general systems) for different orderings, reduced-row Echelon forms are different and also reduced GBs are different

Example: To illustrate this for a system of linear equations we have to consider less equations than unknowns

$$\begin{bmatrix} 2 & 4 & 2 & 1 & 7 \\ 2 & 4 & 1 & 2 & 8 \\ 1 & 2 & 3 & 1 & 4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad \text{RREF} \quad \begin{bmatrix} 1 & 2 & 0 & 0 & 3 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Different ordering

$$\begin{bmatrix} 2 & 1 & 7 & 2 & 4 \\ 1 & 2 & 8 & 2 & 4 \\ 3 & 1 & 4 & 1 & 2 \end{bmatrix} \begin{bmatrix} x_3 \\ x_4 \\ x_5 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \quad \text{RREF} \quad \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -\frac{1}{3} & -\frac{2}{3} \\ 0 & 0 & 1 & \frac{1}{3} & \frac{2}{3} \end{bmatrix}$$

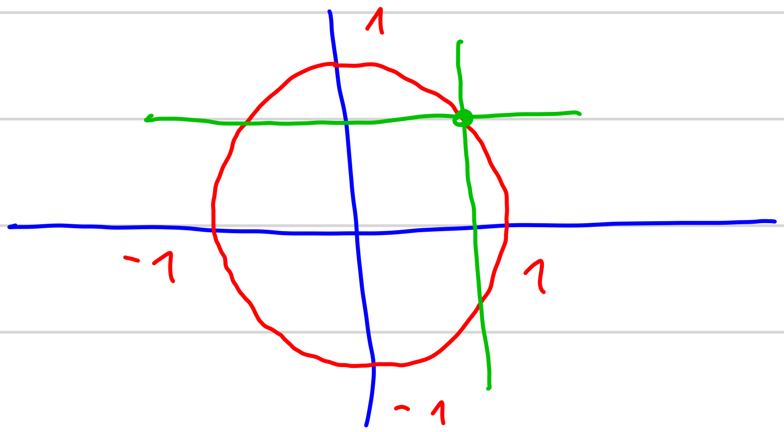
- The reduced-row Echelon form is <u>unique</u> for a <u>given order</u> of unknowns and it provides the reduced GB

- Matrix of the RREF w.r.t one ordering is <u>not equal</u> to the matrix of the RREF w.r.t. another ordering and the corresponding reduced GB are also different

Several non-linear polynomial eq. in several unknowns

- Technique for transforming a system of polynomial equations with a finite number of solutions into a system that will contain a polynomial in the "last" unknown say x_n

$\Rightarrow$ will allow for solving for x_n and reducing the problem from n to $n-1$ unknowns and so on until we solve for all unknowns



Example:

$$f_1 = x_1^2 + x_2^2 - 1 = 0$$
$$f_2 = 25x_1x_2 - 20x_2 - 15x_1 + 12 = 0$$

Matrix form:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 25 & -20 & 0 & -15 & 12 \end{bmatrix} \begin{bmatrix} x_2^2 \\ x_1x_2 \\ x_2 \\ x_1^2 \\ x_1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

$f = 0 \Rightarrow f \cdot g = 0$ for any $g \in \mathbb{Q}[x_1, x_2]$

e.g. $x_1 \cdot f_1 = 0$, $x_2 \cdot f_2 = 0$

- Adding "new equations" of the form $f_i \cdot g = 0$ to the original system produces a new system with the same solutions

- Polynomials f, $x.f$ are linearly independent when $f \neq 0$ since $x.f$ has degree strictly greater than is the degree of f
$\Rightarrow$ by adding $x.f$ $(g.f)$ we have a chance to add another independent row to the matrix

- Let's add $x_1 f_1$, $x_2 f_2$ to our system and write it in the matrix form

$$\begin{array}{c} \\ f_1 \\ f_2 \\ x_1 f_1 \\ x_2 f_2 \end{array} \begin{array}{c} \begin{array}{cccccccc} x_1x_2^2 & x_2^2 & x_1x_2 & x_2 & x_1^3 & x_1^2 & x_1 & 1 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 25 & -20 & 0 & 0 & -15 & 12 \\ 1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 25 & -20 & -15 & 12 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

- more rows have been added but also new monomials $x_1x_2^2$ and x_1^3

Eliminate it by the Gaussian elimination

$$\begin{array}{cccccccc} x_1x_2^2 & x_2^2 & x_1x_2 & x_2 & x_1^3 & x_1^2 & x_1 & 1 \end{array}$$
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 25 & -20 & 0 & 0 & -15 & 12 \\ 0 & 0 & 0 & 0 & -125 & 100 & 80 & -64 \end{bmatrix}$$

the last row gives an equation in single unknown y

- We have been ordering monomials corresponding to the columns of the matrix such that we have all monomials in y at the end

- It can be shown that similar procedure works for every system of polynomial equations $\{f_1, \dots, f_k\} \in \mathbb{Q}[x_1, \dots, x_n]$ with a finite number of solutions

In particular, there always are n finite sets M_i, $i = 1, \dots, n$ of monomials such that the extended system

$$\{f_1, f_2, \dots, f_n\} \cup \{m.f_j \mid m \in M_j, \ j = 1, \dots n\}$$

has matrix A with the following nice property:

- If the last columns of A correspond to all monomials in a single unknown x_i (y) (including 1), then the last non-zero row of matrix B, obtained by the Gassian elimination of A produces a polynomial in single unknown x_i (y)

- a very powerful technique
- a tool how to solve all systems of polynomial equations with a finite number of solutions

- In practice the main problem is how to find small sets M_i in acceptable time

- the number of monomials of total degree at most d in n unknowns is given by the combination number $\binom{n+d}{d}$

  $\Rightarrow$ the size of the matrix A is growing very quickly

- Practical algorithms (e.g. F4), use many tricks how to select small sets of monomials and how to efficiently compute in exact arithmetics over $\mathbb{Q}$